"Snapshots" Capture Cyber Threats

In accordance with the South Carolina Strategy for Homeland Security, several cyber target capabilities have been identified and are currently under development by South Carolina Information Sharing and Analysis Center (SC-ISAC). One such development is a cyber attack response solution known as "Trusted Enterprise Service." This new service, now available for participating agencies, will provide increased security to systems, networks and data by remotely analyzing and reporting "snapshots" of volatile data running on agency systems. The volatile data collected consists of user information, port information, open files and all running processes.

Jim MacDougall, Chief Security Officer, directs the services of the South Carolina Information Sharing and Analysis Center (SC-ISAC).

By comparing these snapshots, SC-ISAC can show all machines that have been compromised during an intrusion or show the spread of a virus and where it originated. This unique ability to audit large groups of machines for unauthorized processes will allow SC-ISAC to respond immediately to any previously undiscovered cyber attack. Any hidden or unauthorized process can be detected and removed including spyware, malware, viruses, Trojans, keyloggers, adware, rootkits or hacking tools. After an unauthorized process has been discovered, it is investigated and all malicious codes identified. This knowledge can be used to create a script that can kill and delete any process across a Wide Area Network.

Through Trusted Enterprise, participating agencies will be able to benefit from access to the:

- Only available commercial solution that can find and remediate Windows-based rootkits.
- Only truly secure and scalable network-enabled forensic investigation platform in existence.
- Only tool that can investigate systems without firewall changes anywhere in the world.
- Only solution that can cleanly kill and delete any process across a Wide Area Network.

Trusted Enterprise is only one of the many steps SC-ISAC has implemented to help ensure that federal, state, county and local government systems are secure and protected from the potential ramifications of cyber terrorist activities.

For additional information on Trusted Enterprise, please visit the CIO Web site.

About SC-ISAC

The South Carolina Information Sharing and Analysis Center (SC-ISAC), led by Chief Security Officer James MacDougall, is a unique partnership designed to detect, preempt and prevent future cyber terrorist acts while also analyzing and distributing information on security events, best practices and awareness programs to federal, state, county and local governments.

These efforts are supported through the combining of resources such as personnel, equipment and information from the Division of the State Chief Information Officer (CIO), the South Carolina Law Enforcement Division (SLED), the United States Secret Services, the Multi-State ISAC, the United States Computer Emergency Readiness Team (US-CERT) and the Department of Homeland Security.

For additional information on SC-ISAC, please visit the Secure South Carolina Web site.